

REMARKS

Applicant is hereby voluntarily amending claims 1, 7, and 12; and canceling claims 3 and 4. Support for all amendments is found in the application as originally filed, particularly Figure 8 and accompanying description. Reconsideration of this application as amended, and allowance of all claims remaining herein, claims 1, 2, 5-14 and 18-86 as amended, are hereby respectfully requested.

Examiner Colin granted a telephonic interview to the undersigned on August 22, 2006. During said interview, the claims were discussed, but no agreement was reached concerning the patentability of any claims. No exhibit was shown, nor was any demonstration conducted. During the interview, it was decided that Applicant would submit a voluntary amendment that would clarify the language of the claims and remove some of the issues involved in this prosecution. Applicant is hereby submitting this Amendment E as that voluntary amendment. Amendment E uses Amendment D as a base. Thus, the Examiner should first enter Amendment D and then enter Amendment E. Please note that in Amendment D, claim 68 should have been labeled "currently amended" rather than "previously presented".

The Examiner's attention is drawn to the additional proposed drawing corrections and amendments proposed in Amendment D. The Examiner is again asked to approve these corrections and amendments. Other than the section pertaining to these drawing corrections and amendments, the Examiner can ignore the Remarks section of Amendment D, and rely upon the Remarks section of this Amendment E instead.

In the third paragraph of his Office Action mailed January 25, 2006, the Examiner rejected claims 1-17 under 35 U.S.C. §103(a) as being unpatentable over Orrin in view of Shear. Applicant is hereby canceling claims 3 and 4; and amending independent claim 1 (the only independent claim in this set of rejected claims) and dependent claims 7 and 12 to highlight novel aspects of his invention. Note that claim 1's "first user computer" reads on relying customer 108 of Figure 1, and that claim 1's "second user computer" reads on subscribing customer 106 of Figure 1, i.e., in claim 1, "first" and "second" are interchanged with respect to the most common phraseology used in Applicant's specification.

As amended, Applicant's claims are patentably distinct over the cited references for, inter alia, the following reasons:

1. Orrin is remote, because Orrin does not affix a digital signature to anything that is executable. The only thing that Orrin affixes a digital signature to is non-executable data. On the other hand, Applicant's claim 1 recites that the second digital signature is affixed to at least one executable component running in an environment of the executable browser software.

Applicant could just as easily have used the expression "executed upon" as "affixed to".

Orrin's paragraph 39 makes it clear that his digital signature is affixed to content (data), not to executable browser software. In paragraph 39, Orrin states: "In step 246, obligor 102 performs a signing function on the content... many internet browsers have signature functions as built-in features... The resulting combination of content 212, timestamp 214, and obligor's signature 216 forms signed content 210. Signed content 210 may then be sent to trusted server 100, for example, using an HTTP post operation." (emphasis added)

2. In Applicant's claims, authenticating the second digital signature, which vouchsafes the executable Web browser software, occurs subsequent to the browser having doubly digitally signed the electronic document, i.e., subsequent to execution of the executable Web browser software. This is now clear in view of the words "subsequent to" that Applicant is adding to claim 1 in this Amendment E. Support for this recitation is found in Applicant's specification at, inter alia, page 10 line 21 through page 11 line 26.

Shear, on the other hand, teaches away from the present invention in that the comparison of hashes of his executable load module is performed before the executable load module executes. To verify the trustworthiness of the load module after its execution would be contrary to the purpose of Shear, which is to validate the trustworthiness of the load module prior to its running in a protected processing environment. Such a system is used to insure that the load module has not been tampered with prior to its operation, in order to avoid executing a compromised program. Applicant's invention is not concerned with the validity of an executable program to be run in the future (such as Shear's load module). Rather, Applicant's invention is concerned with determining the validity of a digitally signed document or transaction by ensuring the validity of the signature and the trustworthiness of the browser that digitally signed the document or initiated the transaction in the past. This is unexpected in view of Shear.

3. The cited references, whether taken alone or in combination, do not suggest claim 1's recitation of a first digital signature that is affixed to a combination comprising content plus a second digital signature. This recitation is supported by Applicant's Figure 8 and accompanying description. Figure 8 illustrates three embodiments. Each embodiment features a first digital signature affixed to a combination of content (the "purchase order" of Figure 8) plus a second digital signature (the block of each embodiment of Figure 8 entitled "digital signature of each signed component running in the browser environment").

Claims 2 and 5-14 depend upon independent claim 1, and therefore the patentability of these dependent claims flows from the patentability of claim 1.

Further with respect to claim 7, the "combination further comprises a hash" recitation of claim 7 is not suggested by the prior art, whether taken alone or in combination. Claim 7 tracks the bottom of the three embodiments illustrated in Figure 8.

Further with respect to claim 12, the "combination further comprises an unsigned executable component" recitation of claim 12 is not suggested by the prior art, whether taken alone or in combination. The embodiment recited in claim 12 is illustrated as the middle and bottom embodiments of Figure 8.

For the above reasons, the Examiner is requested to withdraw his rejection of claims 1-17; and to allow claims 1, 2, and 5-14 as amended. (Claims 15-17 were canceled in Amendment D).

In the fourth paragraph of his Office Action mailed January 25, 2006, the Examiner rejected claims 18-86 under 35 U.S.C. §103(a) as being unpatentable over Shear in view of Sudia.

In this rejected claim set, the independent claims are claims 18, 35, 50, and 68.

As amended, claims 18-86 are patentable for, inter alia, the following reasons:

Independent claims 18 and 35 are directed to verifying the trustworthiness of an executable Web browser. Sudia discusses a "browser" doing a vague "certificate handshake" with a web server (paragraphs 0401 through 0434), but Sudia does not suggest verification of the executable Web browser code itself, which is the subject matter of Applicant's claims. Furthermore, Sudia does not suggest taking the hash values that are recited in Applicant's claims.

Additionally, the only one of these references that treats the authentication of executable code, Shear, does not suggest the recitation of claims 18 and 35 that the determination of the trustworthiness of the executable Web browser is performed subsequent to the browser having executed (by virtue of its having digitally signed an electronic document).

Shear teaches away from the present invention in that the comparison of hashes of his executable load module is performed before the executable load module executes. To verify the trustworthiness of the load module after its execution would be contrary to the purpose of Shear, which is to validate the trustworthiness of the load module prior to its running in a protected processing environment. Such a system is used to insure that the load module has not been tampered with prior to its operation, in order to avoid executing a compromised program. Applicant's invention is not concerned with the validity of an executable program to be run in the future (such as Shear's load module). Rather, Applicant's invention is concerned with determining the validity of a digitally signed document or transaction by ensuring the validity of the signature and the trustworthiness of the browser that digitally signed the document or initiated the transaction in the past. This is unexpected in view of Shear.

Thus, the combination of Sudia and Shear does not suggest Applicant's claimed invention.

Dependent claims 19-34 and 36-49 depend upon independent claims 18 and 35, respectively. Therefore, the patentability of claims 19-34 and 36-49 flows from the patentability of claims 18 and 35.

Further with respect to dependent claims 22, 23, 39, and 40, neither Shear nor Sudia suggests the "unknown" status of a Web browser as recited in said claims.

Further with respect to dependent claim 24, neither Shear nor Sudia suggests the step of receiving from a requestor a request to determine the trustworthiness of a Web browser module, the request including a second set of hashes, as recited in claim 24.

Further with respect to dependent claims 46-49, neither Shear nor Sudia suggests the first customer, second customer, transaction, buyer relationship, or seller relationship recited in said claims.

Independent claims 50 and 68 recite a four-corner trust model comprising a root entity, a first participant, a second participant, a first customer of the first participant, and a second customer of the second participant. The two cited references are remote, because they neither mention nor suggest these five specific recited entities.

Also, all of claims 50-86 recite that the second set of hashes is transmitted by the first customer to the second customer, using a network connection. Neither Shear nor Sudia suggests transmitting hashes anywhere. Shear's hash comparisons are performed at the same microprocessor; Sudia does not use hashes to authenticate code.

Additionally, the references do not suggest the set of hashes recited in all of claims 50-86. Shear sometimes performs several different verifications on the same load module, but for each verification of an executable load module, Shear takes just one hash.

Furthermore, the references do not suggest the trusted verifier module recited in claims 50 and 68; or the detailed generating, transmitting, forwarding, and determining steps recited in claim 50; or the corresponding "means for" elements recited in claim 68.

Claims 51-67 and 69-86 depend upon independent claims 50 and 68, respectively. Therefore, the patentability of claims 51-67 and 69-86 flows from the patentability of claims 50 and 68.

Further with respect to dependent claims 53, 56, 71, and 75, neither Shear nor Sudia suggests the "unknown" browser status recited in these claims.

Further with respect to dependent claims 57, 58, 59, 76, 77, and 78, neither Shear nor Sudia suggests the transaction recited in these claims.

Further with respect to dependent claims 60 and 79, neither Shear nor Sudia suggests the root entity operating rules recited in these claims.

Further with respect to dependent claims 63, 64, 82, and 83, neither Shear nor Sudia suggests the transaction coordinator recited in these claims.

Further with respect to dependent claims 65, 66, 84, and 85, neither Shear nor Sudia suggests the integration of a trusted verifier module into another component as recited in these claims.

For the above reasons, the Examiner is requested to withdraw his rejection of claims 18-86; and to allow these claims as amended.

Applicant believes that this application is now in condition for allowance of all claims remaining herein, claims 1, 2, 5-14 and 18-86 as amended, and therefore an early Notice of Allowance is respectfully requested. If the Examiner disagrees or believes that for any other reason, direct contact with Applicant's attorney would help advance the prosecution of this case to finality, he is invited to telephone the undersigned at the number given below.

Respectfully submitted,

date of signature: *Sept- 18, 2006*



Edward J. Radlo
Attorney Under Rule 34
Reg. No. 26,793

SONNENSCHN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, IL 60606-1080
Tel.: (415)882-2402

cc: IP/T docket CH
L. Miller (via e-mail)
K. Ruthenberg

27246800V-4